UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/992,823	11/14/2001	Daniel W. Wong	1376-0100520	5879

34456 7590 02/19/2008

LARSON NEWMAN ABEL POLANSKY & WHITE, LLP
5914 WEST COURTYARD DRIVE
SUITE 200
AUSTIN, TX 78730

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
02/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/992,823	WONG ET AL.	
	Examiner	Art Unit	
	LONGBIT CHAI	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47,49-54,63 and 64* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) *25* is/are allowed.

6)☒ Claim(s) *1-24, 26-47,49-54,63 and 64* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Currently pending claims are 1 – 47, 49 – 54 and 63 – 64.

Response to Arguments

2. Applicant's arguments with respect to the pre-appeal filed on 12/21/2007 have been fully considered but are moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 13, 31, 40, 41, 47, 49, 50 and 52 are rejected under 35 U.S.C. 102(e) as being anticipated by Daellenbach et al. (U.S. Patent 2003/0168508).

As per claim 1, 31, 40, 47 and 49, Daellenbach teaches a method comprising the steps of:

sending a first encrypted routine of a software driver to a peripheral device (Daellenbach: Para [0069] Line 10 – 11 / Line 13 – 15): (a) the driver software can be download and (b) the encrypted driver software is indeed a driver software (i.e. routine) which is encrypted

and can be used by a software driver after being decrypted), **wherein the software driver is to interface with the peripheral device** (Daellenbach: Para [0069] Line 15);

decrypting, at the peripheral device, the first encrypted routine to generate a plaintext routine (Daellenbach: Para [0069] Line 10 – 11 / Line 13 – 15: (a) the download encrypted driver software must be decrypted so that it can be used to perform driver function (b) the encrypted driver software after being decrypted is qualified as a plaintext routine); and

providing the plaintext routine to the software driver (Daellenbach: Para [0069] Line 10 – 11: i.e. the purpose of downloading the driver software).

As per claim 13, Daellenbach teaches selecting the first encrypted routine from a plurality of different encrypted routines, wherein the plurality of different encrypted routines are functionally equivalent (Daellenbach: Para [0069] Line 10 – 11: the routines used for the purpose of driver software updates are indeed being selected from a plurality of driver routines with different revisions).

As per claim 41, Daellenbach teaches said first interface and said second interface are implemented using a same interface (Daellenbach : Para [0069] Line 10 – 11 / Line 13 – 15): the encrypted driver software being download can be used by a software driver after being decrypted at the same interface entity).

As per claim 50, Daellenbach teaches the first encrypted data includes an encrypted software routine (Daellenbach : Para [0069] Line 13 – 15).

As per claim 52, Daellenbach teaches the application includes a software driver (Para [0069] Line 13 – 15).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1 – 3, 8 – 9, 13, 16, 31, 33, 38, 40, 47, 49, 51, 63 and 64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carter (U.S. Patent 7,000,106), in view of Ciacelli (U.S. Patent 6,236,727).

As per claim 1, 31, 40, 47 and 49, Carter teaches a method comprising the steps of:

sending a first encrypted routine (see Ciacelli below) **of a software driver to a peripheral device** (Carter: Column 9 Line 26 – 30 and Column 6 Line 56 – 58: downloading encryption / decryption routines to a software driver), **wherein the software driver is to interface with the peripheral device** (Carter: Column 6 Line 57 – 58).

However, Carter does not explicitly teaches the encryption / decryption routines, when downloaded, is in an encrypted form).

Ciacelli teaches the encryption / decryption routines, when downloaded, is in an encrypted form (Ciacelli: Column 5 Line 43 – 45).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ciacelli within the system of Carter because (a)

Carter discloses downloading encryption / decryption routines to a software driver in a secured kernel mode environment (Carter: Column 9 Line 26 – 30 and Column 2 Line 20 – 26) and (b) Ciacelli teaches a security enhanced mechanism to transfer / download the decryption / encryption routines to a device by encrypting the routine content (Ciacelli: Column 5 Line 43 – 45).

decrypting, at the peripheral device, the first encrypted routine to generate a plaintext routine (Ciacelli: Column 5 Line 46 – 48: decrypting at the hardware device 27) & (Carter: Column 9 Line 26 – 30: (a) the download encrypted driver software must be decrypted so that it can be used to perform driver function (b) the encrypted driver software after being decrypted is qualified as a plaintext routine); and

providing the plaintext routine to the software driver (Carter: Column 9 Line 26 – 30: i.e. the purpose of downloading the driver software).

As per claim 2, Carter as modified teaches the first encrypted routine is an encrypted version of an encryption routine (Carter: Column 6 Line 57 – 58 and Column 2 Line 20 – 26 & Ciacelli: Column 5 Line 43 – 45 / Line 53 – 60: (a) Carter is relied upon to download an encryption routine to a software driver in a secured kernel mode environment (b) Ciacelli is relied upon to provide an secured means to download decryption / encryption algorithm to a peripheral device by encrypting the routine content).

As per claim 3, Carter as modified teaches the first encrypted routine is an encrypted version of a decryption routine (Ciacelli: Column 5 Line 43 – 45).

As per claim 8, 33 and 38, Carter as modified teaches sending a decryption code to the peripheral device, where the decryption code is to be used by the peripheral device to decrypt the first encrypted routine (Ciacelli: Column 5 Line 45 – 60).

As per claim 9, Carter as modified teaches removing the plaintext routine (Ciacelli: Column 7 Line 16 – 21).

As per claim 13, Carter as modified teaches selecting the first encrypted routine from a plurality of different encrypted routines, wherein the plurality of different encrypted routines are functionally equivalent (Ciacelli: Column 5 Line 53 – 60: the routines used for the purpose of driver software updates are indeed being selected from a plurality of driver routines with different revisions).

As per claim 16, Carter as modified teaches providing includes storing the plaintext routine in a location in memory accessible by the software driver, and where the location in memory is known to the software driver (Carter: Column 9 Line 26 – 30: the "encryption / decryption routine" after being downloaded must be, first, stored in the memory somewhere and secondly, must be known to the software driver so that the encryption / decryption algorithm functions can be performed and executed accordingly to encrypt / decrypt the data).

As per claim 51, Carter as modified teaches the first encrypted data includes an encrypted version of one of: a private encryption key, a private decryption key, a chip ID, and a device ID (Ciacelli: Column 6 Line 42 – 45).

As per claim 63, Carter as modified teaches processing data at the peripheral device using the plaintext routine (Carter: Column 9 Line 26 – 30: encryption / decryption driver plaintext routine).

As per claim 64, Carter as modified teaches decrypting data at the peripheral device using the plaintext routine (Ciacelli: Column 5 Line 45 – 60).

5. Claims 2, 3, 8, 33 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daellenbach et al. (U.S. Patent 2003/0168508), in view of Carter (U.S. Patent 7,000,106).

As per claim 2, Daellenbach does not disclose expressly the first encrypted routine is an encrypted version of an encryption routine.

Carter teaches the first encrypted routine is an encrypted version of an encryption routine (Carter: Column 9 Line 26 – 30).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Carter within the system of Daellenbach because (a) Daellenbach discloses downloading driver routines to a software driver (Daellenbach: Para [0069] Line 10 – 11 / Line 13 – 15) and (b) Carter teaches the downloaded software driver can be encryption / decryption routines (Carter: Column 9 Line 26 – 30).

As per claim 3, Daellenbach does not disclose expressly the first encrypted routine is an encrypted version of a decryption routine.

Carter teaches the first encrypted routine is an encrypted version of a decryption routine (Carter: Column 9 Line 26 – 30). See the same rationale of combination applied herein as above in rejecting the claim 2.

As per claim 8, 33 and 38, Daellenbach does not disclose expressly sending a decryption code to the peripheral device.

Carter teaches sending a decryption code to the peripheral device (Carter: Column 9 Line 26 – 30). See the same rationale of combination applied herein as above in rejecting the claim 2.

Daellenbach as modified teaches where the decryption code is to be used by the peripheral device to decrypt the first encrypted routine (Daellenbach: Para [0069] Line 10 – 11 / Line 13 – 15: the encrypted routine after being downloaded must be, first, decrypted so that the downloaded functions can be performed and executed accordingly).

6. Claims 10 – 12, 32, 39, 42, 43 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daellenbach et al. (U.S. Patent 2003/0168508), in view of Hendricks et al. (U.S. Patent 7,298,851).

As per claim 10, 32, 42 and 54, Daellenbach does not disclose expressly encrypting, at the peripheral device, the plaintext routine to generate a second encrypted routine, where the second encrypted routine is a version of the first encrypted routine.

Hendricks teaches encrypting, at the peripheral device, the plaintext routine to generate a second encrypted routine, where the second encrypted routine is a version of the first encrypted routine (Hendricks: Column 63 Line 22 – 26: secure storage is done on a memory device at the driver-level, where all information (i.e. including the driver routine disclosed by Daellenbach) stored on the memory storage device is encrypted by a memory device driver prior to being stored on memory storage device);

providing the second encrypted routine to the software driver (see above – merely for storage purpose (i.e. securely store the content) after being downloaded).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Hendricks within the system of Daellenbach because (a) Daellenbach discloses downloading driver routines to a software driver (Daellenbach: Para [0069] Line 10 – 11 / Line 13 – 15) and (b) Hendricks teaches a secured mechanism to store all information (i.e. including the downloaded content) (Hendricks: Column 63 Line 22 – 26).

As per claim 11 and 39, Daellenbach as modified teaches sending a encryption code to the peripheral device (Daellenbach: Para [0069] Line 10 – 11 / Line 13 – 15), where the encryption code is to be used by the peripheral device to encrypt the plaintext routine (Hendricks: Column 63 Line 22 – 26: encrypting all information prior to storing is indeed including not only data but also routines).

As per claim 12, Daellenbach as modified teaches the second encrypted routine is a modified version of the first encrypted routine (Daellenbach: Para [0069] Line 10 – 11 / Line 13 – 15: (a) updated software driver) & (Hendricks: Column 63 Line 22 – 26: i.e. storage version).

As per claim 43, Daellenbach as modified teaches the first hardware component and the second component are implemented using a same hardware component (Ciacelli: Column 5 Line 43 – 48: the same hardware component of decryption module to receive and execute the decryption function for encrypted routine).

7. Claims 10, 12, 32, 42 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carter (U.S. Patent 7,000,106), in view of Ciacelli (U.S. Patent 6,236,727), in view of Hendricks et al. (U.S. Patent 7,298,851).

As per claim 10, 32, 42 and 54, Carter as modified does not disclose expressly encrypting, at the peripheral device, the plaintext routine to generate a second encrypted routine, where the second encrypted routine is a version of the first encrypted routine.

Hendricks teaches encrypting, at the peripheral device, the plaintext routine to generate a second encrypted routine, where the second encrypted routine is a version of the first encrypted routine (Hendricks: Column 63 Line 22 – 26: secure storage is done on a memory device at the driver-level, where all information (i.e. including the downloaded driver routine disclosed by Carter) stored on the memory storage device is encrypted by a memory device driver prior to being stored on memory storage device);

providing the second encrypted routine to the software driver (see above – merely for storage purpose (i.e. securely store the content) after being downloaded).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Hendricks within the system of carter because (a) Carter discloses downloading driver routines to a software driver (Carter: Column 9 Line 26 – 30) and (b) Hendricks teaches a secured mechanism to store all information – i.e. including the downloaded content (Hendricks: Column 63 Line 22 – 26).

As per claim 12, Carter as modified teaches the second encrypted routine is a modified version of the first encrypted routine (Carter: Column 9 Line 26 – 30) & (Ciacelli: Column 5 Line

43 – 45 / Line 53 – 60: updated encrypted / decryption algorithm routines) & (Hendricks: Column 63 Line 22 – 26: i.e. storage version).

8. Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carter (U.S. Patent 7,000,106), in view of Ciacelli (U.S. Patent 6,236,727), in view of Wilson (U.S. Patent 4,520,232).

As per claim 14, Carter as modified does not disclose expressly decrypting includes using a map as a decryption key.

Wilson teaches decrypting includes using a map as a decryption key (Wilson: see for example: Column 2 Line 12 – 24).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Wilson within the system of Carter as modified because (a) Carter teaches inserting a security algorithm within the kernel such as downloading encryption / decryption algorithm routines to a device driver interfaced with a peripheral device that is implemented including a graphic user interface (GUI) (Carter: Column 2 Line 20 – 26 and Column 10 Line 17 – 21) and (b) Wilson teaches providing a poly-graphic encryption mechanism which is both fast and inexpensive with enhanced security strength (Wilson: see for example, Column 1 Line 28 – 34).

As per claim 15, Carter as modified teaches the map includes a texture map (Wilson: see for example, Column 1 Line 28 – 34: the matrix is qualified as a two-dimensional texture map).

9. Claims 4 – 7, 17 – 24, 26, 27, 30, 34 – 37, 44 – 46 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carter (U.S. Patent 7,000,106), in view of Ciacelli (U.S. Patent 6,236,727), and in view of Freeman (U.S. Patent 2002/0129374).

As per claim 4, 34 and 53, Carter as modified does not disclose expressly the peripheral device is a graphics chip.

Freeman teaches the hardware device is a graphic chip (Freeman: see for example, Paragraph [0117]).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Freeman within the system of Carter as modified because (a) Carter teaches inserting a security algorithm within the kernel such as downloading encryption / decryption algorithm routines to a device driver interfaced with a peripheral device that is implemented including a graphic user interface (GUI) (Carter: Column 2 Line 20 – 26 and Column 10 Line 17 – 21) and (b) Freeman teaches using a graphic chip to realize the MPEG adaptation and to process the video data stream (Freeman: Paragraph [0117] and Figure 7 Element 376 & 388).

As per claim 5 – 6, 35 – 36 and 44 – 45, Carter as modified teaches decrypting is performed by a graphics chip (Ciacelli: see for example: Column 3 Line 25 – 43, Column 5 Line 43 – 60 and Column 2 Line 48 – 50).

Carter as modified does not disclose expressly decrypting is performed by a 3D pipe of the graphics chip.

Carter as modified does not disclose expressly decrypting is performed by a 3D pipe of the graphics chip.

However, it would have been obvious to a person of ordinary skill in the art at the time the invention was made for a modification because 3D (3-Dimension) engine (or IDCT component) is merely one part of a series of video graphic chips in this claimed subject of matter to perform encryption / decryption).

As per claim 7, 37 and 46, Carter as modified teaches decrypting is performed by dedicated encryption hardware of the graphics chip (Ciacelli: see for example: Abstract Line 15 – 17 and Column 2 Line 55 – 63).

As per claim 17, the claim limitations are met as the same reasons as that set forth in the paragraph above regarding to claim 1 and claim 2 (i.e. claim 2 with base claim 1: see Page 5 under Item #4, for example, Carter: Column 6 Line 57 – 58 and Column 2 Line 20 – 26 & Ciacelli: Column 5 Line 43 – 45 / Line 53 – 60: (a) Carter is relied upon to download an encryption routine to a software driver in a secured kernel mode environment (b) Ciacelli is relied upon to provide an secured means to download decryption / encryption algorithm to a peripheral device by encrypting the routine content) with the exception of the feature the **peripheral device is a graphic chip**. However, Freeman teaches the hardware device is a graphic chip (Freeman: see for example, Paragraph [0117]).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Freeman within the system of Carter as modified because (a) Carter teaches inserting a security algorithm within the kernel such as downloading encryption / decryption algorithm routines to a device driver interfaced with a peripheral device that is implemented including a graphic user interface (GUI) (Carter: Column 2 Line 20 – 26 and Column 10 Line 17 – 21) and (b) Freeman teaches using a graphic chip to

realize the MPEG adaptation and to process the video data stream (Freeman: Paragraph [0117] and Figure 7 Element 376 & 388).

As per claim 18, Carter as modified teaches sending a decryption code to the peripheral device, where the decryption code is to be used by the peripheral device to decrypt the first encrypted routine (Ciacelli: Column 5 Line 45 – 60).

As per claim 19 – 20, Carter as modified teaches decrypting is performed by a graphics chip.

Carter as modified does not disclose expressly decrypting is performed by a 3D pipe of the graphics chip.

However, it would have been obvious to a person of ordinary skill in the art at the time the invention was made for a modification because 3D (3-Dimension) engine (or IDCT component) is merely one part of a series of video graphic chips in this claimed subject of matter to perform encryption / decryption).

As per claim 21, Carter as modified teaches decrypting is performed by dedicated encryption hardware of the graphics chip (Ciacelli: see for example: Abstract Line 15 – 17 and Column 2 Line 55 – 63) & (Freeman: see for example, Paragraph [0117]).

As per claim 22, Carter as modified teaches decrypting is performed through a series of components coupled within the graphics chip (Ciacelli: see for example: Column 7 Line 58 – 65) & (Freeman: see for example, Paragraph [0117]).

As per claim 23, Carter as modified teaches removing the plaintext routine (Ciacelli: see for example: Column 7 Line 16 – 21).

As per claim 26, Carter as modified teaches the second encrypted routine is a modified version of the first encrypted routine (Ciacelli: Column 7 Line 24 – 29 and Column 5 Line 55 – 56: the encrypted "decryption / encryption algorithm routines" can be updated changed on a needed basis).

As per claim 27, Carter as modified teaches selecting the first encrypted routine from a plurality of different encrypted routines, wherein the plurality of different encrypted routines are functionally equivalent (Ciacelli: see for example: Column 14 Line 10 – 15).

As per claim 30, Carter as modified teaches providing includes storing the plaintext routine in a location in memory accessible by the software driver, and where the location in memory is known to the software driver (: Column 9 Line 26 – 30: i.e. the purpose of downloading the driver software).

10. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Carter (U.S. Patent 7,000,106), in view of Ciacelli (U.S. Patent 6,236,727), in view of Freeman (U.S. Patent 2002/0129374), and in view of Hendricks et al. (U.S. Patent 7,298,851).

As per claim 24, Carter as modified does not disclose expressly encrypting, at the peripheral device, the plaintext routine to generate a second encrypted routine, where the second encrypted routine is a version of the first encrypted routine.

Hendricks teaches encrypting, at the peripheral device, the plaintext routine to generate a second encrypted routine, where the second encrypted routine is a version of the first encrypted routine (Hendricks: Column 63 Line 22 – 26: secure storage is done on a memory device at the driver-level, where all information (i.e. including the downloaded driver routine disclosed by Carter) stored on the memory storage device is encrypted by a memory device driver prior to being stored on memory storage device);

storing the second encrypted routine in memory in a location known to the software driver (see above – merely for storage purpose (i.e. securely store the content) after being downloaded).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Hendricks within the system of carter because (a) Carter discloses downloading driver routines to a software driver (Carter: Column 9 Line 26 – 30) and (b) Hendricks teaches a secured mechanism to store all information – i.e. including the downloaded content (Hendricks: Column 63 Line 22 – 26).

11. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daellenbach et al. (U.S. Patent 2003/0168508), in view of Carter (U.S. Patent 7,000,106), in view of Freeman (U.S. Patent 2002/0129374).

As per claim 34, Daellenbach does not disclose expressly the peripheral device is a graphics chip.

Freeman teaches the hardware device is a graphic chip (Freeman: see for example, Paragraph [0117]).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Freeman within the system of Daellenbach because (a) Daellenbach discloses a device having universal interface board including ATM graphic user interface (GUI) (Daellenbach: Para [0022] & [0069]) and (b) Freeman teaches using a graphic chip to realize the MPEG adaptation and to process the video data stream (Freeman: Paragraph [0117] and Figure 7 Element 376 & 388).

Allowable Subject Matter

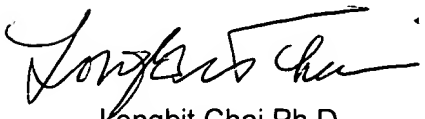
12. Claim 25 is objected to as being dependent upon a rejected base claim but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is an examiner's statement of reasons for allowance: The present invention is directed to a method for sending an encrypted routine of a software driver to a graphics chip, wherein the first encrypted routine is an encrypted version of an encryption routine, and wherein the encryption routine is to be used by the graphics chip to encrypt the plaintext routine. The closest prior art, U.S. Patent 2003/0168508 and U.S. Patent 7,000,106, fail to anticipate or render obvious the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Longbit Chai Ph.D.
Patent Examiner
Art Unit 2131
2/10/2008